GUIDANCE

Denial of Service (DoS) guidance

Guidance to help organisations understand and mitigate DoS attacks.

Pages

- **Denial of Service (DoS) guidance**
- Preparing for denial of service (DoS) attacks +
- A minimal denial of service (DoS) response plan

PUBLISHED
16 March 2016

REVIEWED
25 March 2024

VERSION
1.0

WRITTEN FOR
Large organisations
Public sector
Cyber security professionals
Small & medium sized organisations

iStock.com/Pavel Bezkorovainyi

Who and what is this guidance for?

This guidance helps organisations understand and manage the risk of denial of service (DoS) attacks against a network, system or service, by setting out four essential practices:

1. Understand your service
2. Understand your defences
3. Create a response plan
4. Test your response

It focuses on DoS attacks that originate online. Physical DoS attacks, such as power supply disruption or radio frequency interference, are out of scope. These types of attack should be assessed and managed using business continuity and resilience processes.

What is a DoS attack?

A denial of service (DoS) attack is an attempt to overload a website or network, with the aim of degrading its performance or even making it completely inaccessible.

Typically a successful DoS attack will result in loss of availability of part, or all, of a system, and consume time and money to analyse, defend and recover from.

DDoS attacks

A distributed denial of service (DDoS) attack is a *form* of DoS attack that originates from more than one source. DDoS attacks are typically more effective than attacks from a single source because they usually generate more attacking traffic. The fact that traffic is spread across many sources also makes it harder to distinguish attacker traffic from legitimate traffic.

Where this guidance refers to DoS, it also includes DDoS attacks.

What is the impact?

DoS attacks can easily be targeted against your network, system or service and remain a credible and prevalent threat.

Different types of DoS attack target different parts of a system – for instance, a DoS attack can target a network's capacity to send and receive traffic (its bandwidth), or the processor limitations of servers. The overall impact depends on what is targeted, how long the attack lasts and the effectiveness of your organisational response plan.

Whatever the type of attack, if successful, it will cause the targeted system to become unreliable or unresponsive to a user trying to access it.

For an organisation, an unavailable public-facing website can have a significant impact on an organisation's productivity if it affects business-critical functions. This could include loss of sales, or employees unable to work. This is the case even if an attack is temporary, with no effect on data confidentiality or integrity.

Downloads

Pdf • 151 KB

Prepare for denial of service (DoS) attacks

How to prepare for a denial of service attack and lessen its impact on your organisation.

Next page →
Preparing for denial of service (DoS) attacks

Topics

Configuration management | Secure design and development | Cyber threat | Mitigation

Also see

BLOG POST — 24 May 2024

Raising the cyber resilience of software 'at scale'

New 'Code of Practice for Software Vendors' will ensure that security is fundamental to developing and...

BLOG POST — 20 May 2024

Business email compromise: new guidance to protect your organisation

How to disrupt targeted phishing attacks aimed at senior executives or budget holders.

NEWS — 15 May 2024

NCSC ramps up support for those at high risk of cyber attacks ahead of election

New Personal Internet Protection service provides an extra layer of security on personal devices for high-risk...